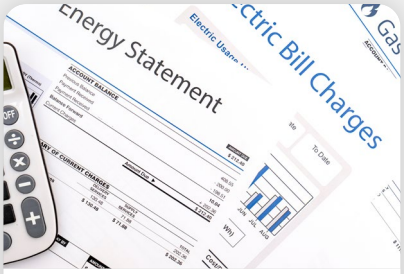
tiaa

FRAUD STOP

Healthcare
Winter 2022

SANCTIONS
What can be applied following an investigation?

→ SEE PAGE 2



SCAM ALERT
Energy scams during the cost of living crisis

→ SEE PAGE 3

BRIBERY ACT COMPLIANCE
What all organisations need to consider

→ SEE PAGE 4

Introduction

The Office for National Statistics say that people are more likely to fall victim to fraud and cyber offences above any other crime. Organisations also face a growing risk of fraud.

The National Crime Agency reports that cyber-crime continues to rise in scale and complexity with the activity affecting essential services and businesses alike. In this edition of Fraud Stop we will be providing insight into real cases along with practical advice and guidance to aid in the identification and prevention of cyber related fraud.

In July 2022, Cifas (the UK's Fraud Prevention Community) predicted that fraud cases were set to soar amidst the cost of living crisis as criminals bet on economic uncertainty.

This edition also considers how the rise in the cost of living is providing criminals with new opportunities to steal personal and financial information. The impact of this activity is increased pressure on individuals and businesses. The potential for individuals to rationalise their behavior along with the increased pressure and potential increased opportunity creates the perfect environment for fraudulent activity.

Sanctions: What can happen following an investigation?

More serious cases are referred to the Crown Prosecution Service for a charging decision. Below are details of two cases concerning an NHS worker and a patient who have been prosecuted in the last six months.

An NHS agency worker was sentenced to nine months imprisonment at Crown Court in May 2022 after earlier pleading guilty to various charges. The worker had worked under a false identity at an NHS Trust as a clinical support worker via an agency between December 2020 and June 2021. They then returned to work at the Trust via a different agency in December 2021. A member of staff flagged the discrepancy and a check of Trust records by an NHS fraud specialist identified two agency worker records with different IDs for the same person. The Home Office (Immigration Enforcement) continued the investigation and the worker was arrested for offences relating to fraud, possession and use of false identity documents and obtaining leave to remain in the UK by deception.

NHS Resolution pursued committal proceedings on behalf of an NHS Trust in line with its strategy to combat and deter fraud by dishonest claimants. In May 2022, a patient was sentenced to six months in jail for deliberately attempting to defraud the NHS in excess of £4 million. They were also ordered to pay back £45K of interim payments, and meet the Trust's costs of the committal application. The court found that the patient has knowingly exaggerated the effect of injuries sustained from a delay in diagnosing spinal cord compression, arising from care provided in 2011. They claimed to have mobility issues and use a crutch, but video surveillance showed them walking normally without assistance.

Police Cautions:

A police caution is a formal alternative to prosecution for less serious cases. You have to admit an offence and agree to be cautioned, and you can be charged if you don't agree to accept a caution. Cautions can show on standard and enhanced Disclosure and Barring Service (DBS) checks. A conditional caution is when conditions are set, and typically this is repayment of any monies lost to the organisation within a set time period. TIAA Anti-Crime Specialists (ACS) have investigated cases which have resulted in cautions being accepted and aside are three examples of these cases.

A healthcare assistant who worked in the community worked in a local Care Home when they were rostered to undertake NHS shifts, being paid for both jobs at the same time. Although it was only five shifts that overlapped, the NHS Trust where they worked has a zero tolerance policy to fraud and a full investigation took place. The healthcare assistant was interviewed under caution and subsequently accepted a conditional caution which was administrated by the police. Their overpaid salary had to be repaid in full within 16 weeks.

A band 7 nurse practitioner was investigated for working for a secondary employer while off sick from their NHS job on three different occasions. The secondary employment was via a nursing agency and 41 shifts were completed while off sick in total. Following the interview under caution, the nurse accepted a conditional caution with the conditions being to reimburse the Trust for the amount of salary overpayment, together with a letter of apology. The Trust was reimbursed in full for the amount of £8,308.74.

A TIAA ACS received an allegation that an NHS administrator had obtained the login details, including the password for a senior member of staff and had accessed the E-rostering system to add themselves to shifts that they had not worked. An investigation substantiated the allegation that had been made and established that the fraudulent hours claimed amounted to £7,571.82. The administrator attended an interview under caution where they admitted the fraud. Following the interview, the administrator accepted a police conditional caution and agree to repay the NHS Trust in full and write a letter of apology. Internal action also resulted in a dismissal.

Scam alerts during the cost of living crisis

Action Fraud, the National Fraud and Cyber Crime Reporting Centre, has issued a warning about the following scam currently in circulation:

Criminals are exploiting the cost of living crisis and targeting the public with energy rebate scams. 1500 reports have been made to the National Fraud Intelligence Bureau regarding scam emails about energy rebates purportedly from Ofgem, the independent energy regulator. The scam emails claim that the recipient is due a rebate payment as part of a government scheme and provides links for the recipient to follow to apply for the rebate. The links lead you to malicious websites designed to steal your personal and financial information. The subject header of the emails states "Claim your bill rebate now" and the Ofgem logo and colours are used so that the email appears authentic.

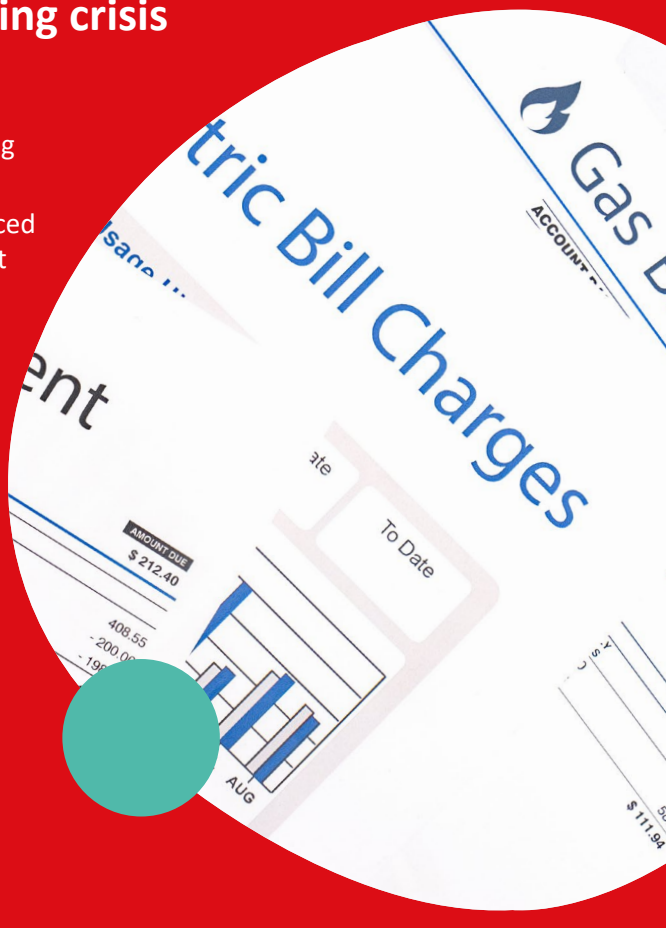
This is an example of authorised push payment scams when criminals trick you into sending money directly from your account to an account controlled by the criminal.

REMEMBER:

- **STOP - Take a moment to stop and think before parting with your money and giving out information**
- **CHALLENGE - It could be fake, so it is OK to refuse any request. Only criminals will try to rush you**
- **PROTECT - Contact your bank immediately if you think you have been a victim of a scam and report it to Action Fraud**
  Reporting fraud and cyber crime

Similar frauds relating to the cost of living crisis include:

- Texts or emails from your energy supplier similarly diverting you to malicious websites.
- Prepayment meter tokens being cloned and sold at a reduced price, but your energy supplier never receives the payment and the tokens are fake.
- Scammers offering better fixed rate deals if you switch urgently – the scammers will be after your bank details.
- Energy saving devices being sold online claiming to cut your monthly bills. They are unlikely to work and are also a safety hazard.



Bribery Act Compliance

It is a requirement under the Bribery Act 2010 that organisations should have adequate procedures in place to prevent bribery, and a robust policy should cover as a minimum declarations/conflicts of interest, gifts and hospitality, record keeping and business conduct standards.

In addition for those healthcare organisations that complete a Counter Fraud Functional Standard Return (CFFSR), component 12 requires that: "The organisation has a managing conflicts of interest policy and registers that include gifts and hospitality with reference to fraud, bribery and corruption, and the requirements of the Bribery Act 2020. The effectiveness of the implementation of the process and staff awareness of the requirements of the policy are regularly tested".

TIAA Anti-Crime Specialists can assist in developing a robust anti-bribery policy and procedures for your organisation. For further advice contact Melanie Alflatt, Director, Risk & Advisory – contact details below.

CONSIDER:

- **Proportionality: The action you take should be proportionate to the risks you face and the size of your business.**
- **Top level commitment: Those at the top of an organisation are in the best position to ensure their organisation conducts itself without bribery.**
- **Risk assessment: Think about the bribery risks you might face given the specific context of your organisation, its activities and areas of operation.**
- **Due diligence: Knowing exactly who you are dealing with can help to protect your organisation from taking on people who might be less than trustworthy.**
- **Communication: Communicating your policies and procedures to volunteers, staff and partners will enhance awareness and help to deter bribery.**
- **Monitoring and review: The risks you face and the effectiveness of your procedures may change over time.**

Social Media – Dos and Don'ts when reporting fraud

Social media is typically used for social interaction and access to news, information and decision making and has rapidly become part of daily activity. It is a valuable communication tool locally and worldwide, as well as to share, create, and spread information. It is therefore important to bear in mind what you should and should not do when using social media in relation to reporting an allegation of fraud to your ACS or to the NHSCFA.

Don't:

- DO NOT tag your ACS, TIAA or the NHSCFA in a LinkedIn, Facebook or Twitter post to report an allegation. This does not constitute making a report. These are not the appropriate platforms to report an allegation and are not monitored 24/7
- DO NOT share images of your report or any evidence online on social media
- DO NOT share details of the allegation, including names on social media

Do

- Report online via the recommended reporting lines only (see below)
- Contact only the named person you have been provided contact details for to discuss your concerns, for example your ACS

Everyone has a part to play in fighting fraud. If you suspect any fraud, bribery or corruption against a healthcare organisation, contact your Anti-Crime Specialist.

- **Melanie Alflatt, Director - Risk and Advisory, Email:** fraud@tiaa.co.uk
- **Alternatively, call** the 24-hour reporting line on **0800 028 4060** or use the online reporting form: Report NHS fraud | Help fight fraud within the NHS | Report your fraud concerns and suspicions using a confidential online form (cfa.nhs.uk). All reports are treated in confidence and you have the option to remain anonymous.